THAT WHICH IS CLAIMED IS:

1. A method of determining random values for an stream cipher, comprising:

determining at least two sequential random values in parallel utilizing a common S-box.

2. The method of Claim 1, wherein the step of determining at least two sequential random values in parallel utilizing a common S-box further comprises the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and accesses of the common S-box utilized to determine a second of the two sequential random values; and .

modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

3. The method of Claim 2, wherein the step of determining if a collision exists comprises the steps of:

determining a state associated with the determination of the at least two sequential random values;

comparing values of counters utilized determining the at least two sequential random values; and

detecting a collision based on the determined state and the compared values.

4. The method of Claim 3, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the step of detecting a collision comprises the steps of:

detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

detecting a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

detecting a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

5. The method of Claim 4, wherein the step of modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box comprises the steps of:

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

6. The method of Claim 2, further comprising the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values; and

determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the second of the two sequential random values.

7. The method of Claim 6, wherein the step of determining if a collision exists comprises the steps of:

determining a state associated with the determination of the at least two sequential random values;

comparing values of counters utilized determining the at least two sequential random values; and

detecting a collision based on the determined state and the compared values.

8. The method of Claim 7, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the steps of determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values and determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the second of the two sequential random values comprises the steps of:

detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

detecting a second collision if the determined state is the second state and the second t counter values equals the second i counter value.

9. The method of Claim 8, wherein the step of modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box comprises the steps of:

utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.

10. A system for determining sequential random values in parallel comprising:

a multi-access memory which contains S-box values;

a collision detection/number generation circuit which carries out parallel determinations for at least two sequential random values utilizing the S-box values; and

a state machine circuit operably associated with the collision detection/number generation circuit which controls the sequence of the determination of the sequential random values.

11. The system of Claim 10, wherein the collision detection/number generation circuit is configured to include an i counter containing a value i[n] and a j counter containing a value j[n] and wherein the collision detection/number generation circuit is further configured to, responsive to the state machine being in state 0 initiate a read operation of the multi-access memory device from addresses i[n]+1 and i[n]+2;

responsive to the state machine being in state 1, receive the values of S[i[n]+1] and S[i[n]+2] from the multi-access memory, determine values for j[n+1] and j[n+2] utilizing the values from the multi-access memory and the value of j[n], initiate read operations of the multi-access memory at the addresses of j[n+1] and j[n]+2 and initiate write operations to the multi-access memory to write the values of S[i[n]+2] and S[i[n]+1] to addresses j[n+1] and j[n+2] respectively;

responsive to the state machine being in state 2, receive the values of S[j[n+1]] and S[j[n+2]] from the multi-access memory, initiate read operations of the multi-access memory at addresses S[i[n]+1] + S[j[n+1]] and at address S[i[n]+2] + S[j[n+2]], and initiate write operations to write S[j[n+1]] and S[j[n+2]] to addresses i[n]+1 and i[n]+2 respectively; and

responsive to the state machine being in state 3, receive the results of the read operations from addresses (S[i[n]+1] + S[j[n+1]]) and (S[i[n]+2] + S[j[n+2]]) are from the multi-access memory to provide the at least two sequential random values.

12. The system of Claim 11, wherein the collision detection/number generation circuit is further configured to, responsive to the state machine being in state 3, update the values of i[n] and j[n] with the values of i[n]+2 and j[n+2] respectively and initiate read operations from the multi-access memory from addresses i[n]+1 and i[n]+2 utilizing the updated i[n] value.

13. The system of Claim 12, wherein the collision detection/number generation circuit is further configured to compare values utilized to determine the at least two sequential random values and detect a collision based on the state of the state machine and the compared values.

14. The system of Claim 13, wherein the collision detection/number generation circuit is further configured to detect a first collision if the state machine is in state 1 and the value of i[n]+2 equals the value of j[n+1], detect a second collision if the state machine is in state 1 and the value of j[n+2] equals the value of i[n]+1, detect a third collision if the state machine is in state 1 and the value of j[n+2] equals the value of j[n]+1, detecting a fourth collision if the state machine is in state 2 and the value of j[n+2] equals the value of S[i[n]+1] + S[j[n+1]], detect a fifth collision if the state is in state 2 and the value of S[i[n]+2] + S[j[n+2]] equals the value of i[n]+1 and the value of j[n+2] is not equal to the value of i[n]+1, detect a sixth collision if the state machine is in state 2 and the value of i[n]+1 the value of S[i[n]+1] + S[j[n+1]] and detect a seventh collision if the state machine is in state 2 and the value of S[i[n]+2] + S[j[n+2]] equals the value of i[n]+2.

15. The system of Claim 14, wherein the collision detection/number circuit is further configured to utilize the value of S[i[n]+1] as the value of S[i[n]+2] if the first collision is detected, utilize the value of S[j[n+1]] as the value of S[j[n+2]] and prevent writing S[j[n+1]] to the address of i[n+1] if the second collision is detected, utilize the value of S[i[n]+1] as the value of S[j[n+2]] and prevent writing S[i[n]+1] to the address of j[n+1] if the third collision is detected, utilize the value of S[j[n+2]] as the value of S[S[i[n]+1]+S[j[n+1]] if the fourth collision is detected, utilize the value of S[j[n+1]] as the value of S[S[i[n]+2]+S[j[n]+2]] if the fifth collision is detected, utilize the value of S[j[n+1]] as the value of S[S[i[n]+1]+S[j[n+1]] if the sixth

collision is detected and utilize the value of S[j[n+2]] as the value of S[S[i[n]+2]+S[j[n+2]] if the seventh collision is detected.

16. A system for determining random values for an stream cipher, comprising:

a memory containing an S-box; and

means for determining at least two sequential random values in parallel utilizing the S-box.

17. The system of Claim 16, wherein the means for determining at least two sequential random values in parallel utilizing the S-box further comprises:

means for determining if a collision exists between accesses of the S-box utilized to determine a first of the two sequential random values and accesses of the S-box utilized to determine a second of the two sequential random values; and

means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box.

18. The system of Claim 17, wherein the means for determining if a collision exists comprises:

means for determining a state associated with the determination of the at least two sequential random values;

means for comparing values of counters utilized determining the at least two sequential random values; and

means for detecting a collision based on the determined state and the compared values.

19. The system of Claim 18, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein means for detecting a collision comprises:

means for detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

means for detecting a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

means for detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

means for detecting a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

means for detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

20. The system of Claim 19, wherein the means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

means for utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

means for utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

means for utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

21. The system of Claim 17, further comprising:

means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values; and means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values.

22. The system of Claim 21, wherein the means for determining if a collision exists comprises:

means for determining a state associated with the determination of the at least two sequential random values;

means for comparing values of counters utilized determining the at least two sequential random values; and

means for detecting a collision based on the determined state and the compared values.

23. The system of Claim 22, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values and the means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values comprises:

means for detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

means for detecting a second collision if the determined state is the second state and the second t counter values equals the second i counter value.

24. The system of Claim 23, wherein the means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

means for utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.

25. A computer program product for determining random values for an stream cipher, comprising:

a computer readable media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to provide a memory containing an S-box; and

computer readable program code configured to determine at least two sequential random values in parallel utilizing the S-box.

26. The computer program product of Claim 25, wherein the computer readable program code configured to determine at least two sequential random values in parallel utilizing the S-box further comprises:

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first of the two sequential random values and accesses of the S-box utilized to determine a second of the two sequential random values; and

computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box.

27. The computer program product of Claim 26, wherein the computer readable program code configured to determine if a collision exists comprises:

computer readable program code configured to determine a state associated with the determination of the at least two sequential random values;

computer readable program code configured to compare values of counters utilized determining the at least two sequential random values; and

computer readable program code configured to detect a collision based on the determined state and the compared values.

28. The computer program product of Claim 27, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the computer readable program code configured to detect a collision comprises:

computer readable program code configured to detect a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

computer readable program code configured to detect a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

computer readable program code configured to detect a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

computer readable program code configured to detect a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

computer readable program code configured to detect a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

29. The computer program product of Claim 28, wherein the computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

computer readable program code configured to utilize an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

30. The computer program product of Claim 26, further comprising:

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values; and

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values.

31. The computer program product of Claim 30, wherein the computer readable program code configured to determine if a collision exists comprises:

computer readable program code configured to determine a state associated with the determination of the at least two sequential random values;

computer readable program code configured to compare values of counters utilized determining the at least two sequential random values; and

computer readable program code configured to detect a collision based on the determined state and the compared values.

32. The computer program product of Claim 31, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values and the computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values comprises:

computer readable program code configured to detect a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

computer readable program code configured to detect a second collision if the determined state is the second state and the second t counter values equals the second i counter value.

33. The computer program product of Claim 32, wherein the computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

computer readable program code configured to utilize an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.